PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2005-236403
(43)Date of publication of application : 02.09.2005

(51)Int.Cl. H04L 9/32
G06F 12/14
G06F 15/00

(21)Application number : 2004-040182
(22)Date of filing : 17.02.2004

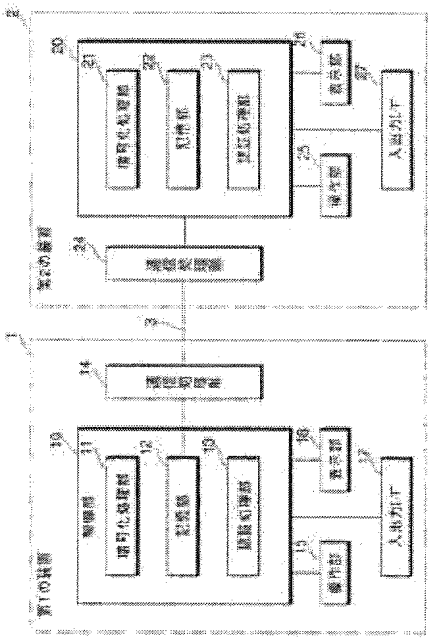
(71)Applicant : TOKYO HOSO:KK
(72)Inventor : SASADA MASAAKI

(54) METHOD AND SYSTEM FOR ELECTRONIC AUTHENTICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an electronic authentication method and an authentication system capable of easily performing the procedure of mutual authentication of electronic information at a low cost between parties concerned without intervention of a third party organization.

SOLUTION: Both a first device (1) and a second device (2) perform first encryption for a plain text by using an encryption key based on an encryption system having exchangeability, and provide and receive the generated encrypted information each other. Next, both the first device (1) and the second device (2) perform second encryption for the encrypted information received from the opposite device by using an encryption key based on an encryption system having exchangeability, and each store the generated encrypted information in their own devices and provide/receive to/from the opposite device. Since both the devices each can obtain the encrypted information obtained by encrypting the information by the own device, and then encrypting by the opposite device and the encrypted information obtained by encrypting the information by the opposite device and then encrypting by the own device; the similarity of the plain texts of both the parties concerned can be authenticated by determining whether the encrypted information matches.



(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-236403
(P2005-236403A)
(43)公開日　平成17年9月2日(2005.9.2)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/32	H04L 9/00	675A	5B017
G06F 12/14	G06F 12/14	320C	5B085
G06F 15/00	G06F 15/00	330E	5J104

審査請求 未請求　請求項の数 8　OL　（全 22 頁）

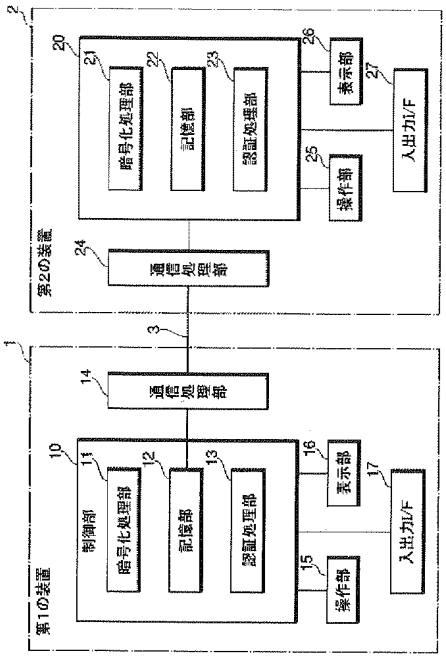
(21)出願番号　特願2004-40182(P2004-40182)
(22)出願日　平成16年2月17日(2004.2.17)

(71)出願人　591084850
株式会社東京放送
東京都港区赤坂５丁目３番６号
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100080953
弁理士　田中　克郎
(74)代理人　100093861
弁理士　大賀　眞司
(72)発明者　笹田　正明
東京都港区赤坂５－３－６　株式会社東京放送内

Fターム(参考)　5B017 AA07 BA05
5B085 AE23 AE29 BG02 CA02 CA04
5J104 LA02 PA07 PA10

(54)【発明の名称】電子認証方法及び電子認証システム

(57)【要約】
【課題】第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことを可能とする電子認証方法及びシステムを提供すること。
【解決手段】平文に対して、第１の装置(1)及び第２の装置(2)の双方が、可換性を有する暗号方式に基づく暗号鍵を用いて１回目の暗号化を行い、生成された暗号化情報を互いに授受する。次に第１の装置(1)及び第２の装置(2)の双方が、相手装置から受け取った暗号化情報に対して、可換性を有する暗号方式に基づく暗号鍵を用いて２回目の暗号化を行い、生成された暗号化情報を自装置に記憶すると共に相手装置と授受する。双方の装置には、自装置が暗号化してその後に相手装置が暗号化して得られた暗号化情報と、相手装置が暗号化してその後に自装置が暗号化して得られた暗号化情報とが得られるので、これらの暗号化情報の一致判定を行うことにより当事者双方の平文の同一性が認証される。
【選択図】　図１



【特許請求の範囲】
【請求項1】
第１の装置と第２の装置との相互間において、互いが有する平文の同一性を認証する電子認証方法であって、
前記第１の装置が、前記平文に対して、可換性を有する暗号方式に基づく第１の暗号鍵を用いた暗号化処理を行って第１の暗号化情報を生成する第１ステップと、
前記第２の装置が、前記平文に対して、可換性を有する暗号方式に基づく第２の暗号鍵を用いた暗号化処理を行って第２の暗号化情報を生成する第２ステップと、
前記第１の装置が、前記第１の暗号化情報を前記第２の装置に送る第３ステップと、
前記第２の装置が、前記第２の暗号化情報を前記第１の装置に送る第４ステップと、
前記第１の装置が、前記第２の装置から取得した前記第２の暗号化情報に対して、前記第１の暗号鍵を用いた暗号化処理を行って第３の暗号化情報を生成して自装置内に記憶する第５ステップと、
前記第２の装置が、前記第１の装置から取得した前記第１の暗号化情報に対して、前記第２の暗号鍵を用いた暗号化処理を行って第４の暗号化情報を生成して自装置内に記憶する第６ステップと、
前記第１の装置が、前記第３の暗号化情報を前記第２の装置に送る第７ステップと、
前記第２の装置が、前記第４の暗号化情報を前記第１の装置に送る第８ステップと、
前記第１の装置が、自装置内に記憶した前記第３の暗号化情報と前記第２の装置から取得した前記第４の暗号化情報とが一致するか否かを判定し、一致する場合に前記平文の同一性が有効であると認証する第９ステップと、
前記第２の装置が、自装置内に記憶した前記第４の暗号化情報と前記第１の装置から受け取った前記第３の暗号化情報とが一致するか否かを判定し、一致する場合に前記平文の同一性が有効であると認証する第１０ステップと、
を含むことを特徴とする電子認証方法。
【請求項2】
前記第３及び第４ステップにおいて、前記第１及び第２の装置のそれぞれは、前記第１及び第２の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合う、請求項１に記載の電子認証方法。
【請求項3】
前記第７及び第８ステップにおいて、前記第１及び第２の装置のそれぞれは、前記第３及び第４の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合う、請求項１に記載の電子認証方法。
【請求項4】
前記第１及び第２の暗号鍵は、前記第１乃至第１０ステップによる一連の認証処理を行う都度に異なる使い捨て鍵である、請求項１乃至３のいずれかに記載の電子認証方法。
【請求項5】
第１の装置と第２の装置との相互間において、互いが有する平文の同一性を認証する電子認証システムであって、
前記第１及び第２の装置のそれぞれは暗号化手段、通信手段、記憶手段及び認証手段を備え、当該第１及び第２の装置が以下のように動作することを特徴とする電子認証システム。
（１）前記第１の装置は、前記暗号化手段により、前記平文に対して、可換性を有する暗号方式に基づく第１の暗号鍵を用いた暗号化処理を行って第１の暗号化情報を生成し、当該第１の暗号化情報を前記通信手段により前記第２の装置に送る。
（２）前記第２の装置は、前記暗号化手段により、前記平文に対して、可換性を有する暗号方式に基づく第２の暗号鍵を用いた暗号化処理を行って第２の暗号化情報を生成し、当該第２の暗号化情報を前記通信手段により前記第１の装置に送る。
（３）前記第１の装置は、前記第２の装置から取得した前記第２の暗号化情報に対して、

前記暗号化手段により前記第１の暗号鍵を用いた暗号化処理を行って第３の暗号化情報を生成して前記記憶手段に記憶するとともに、当該第３の暗号化情報を前記通信手段により前記第２の装置に送る。
（４）前記第２の装置は、前記第１の装置から取得した前記第１の暗号化情報に対して、前記第２の暗号鍵を用いた暗号化処理を行って第４の暗号化情報を生成して前記記憶手段に記憶するとともに、当該第４の暗号化情報を前記通信手段により前記第１の装置に送る。
（５）前記第１の装置は、前記認証手段により、前記記憶手段に記憶した前記第３の暗号化情報と前記第２の装置から取得した前記第４の暗号化情報とが一致するか否かを判定し、一致する場合に前記平文の同一性が有効であると認証する。
（６）前記第２の装置は、前記認証手段により、前記記憶手段に記憶した前記第４の暗号化情報と前記第１の装置から取得した前記第３の暗号化情報とが一致するか否かを判定し、一致する場合に前記平文の同一性が有効であると認証する。
【請求項6】
前記第１の装置の前記通信手段と前記第２の装置の前記通信手段は、それぞれ前記第１及び第２の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合う、請求項５に記載の電子認証システム。
【請求項7】
前記第１の装置の前記通信手段と前記第２の装置の前記通信手段は、それぞれ前記第３及び第４の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合う、請求項５又は６に記載の電子認証システム。
【請求項8】
前記第１及び第２の暗号鍵は、認証処理を行う都度に異なる使い捨て鍵である、請求項５乃至７のいずれかに記載の電子認証システム。

【発明の詳細な説明】
【技術分野】
【0001】
本発明は、複数の当事者間で電子情報について相互認証を行うための電子認証技術に関する。
【背景技術】
【0002】
情報化社会の進展により、従来、紙などの物理的な媒体を用いてやり取りされていた文書（例えば各種の契約書、受領書等）が電子情報に置き換えられつつある。例えば、配送業者が利用者に種々の配送品を届けるような場合を考えると、従来の紙の受領書を介した受領手続きが電子情報の受領書に置き換えられる。またインターネットを介したショッピング等でも同様であり、従来は郵送やファクシミリによって授受されていた注文書が電子情報の注文書に置き換えられる。このように、従来の紙などの物理的媒体を電子情報に代替するには、当該電子情報が複製、改ざん等の不正処理に強いものであることが必要である。このような複数の当事者間における文書等の電子情報の授受手続きにおいて互いの保有する電子情報の認証（正当性の確認）を行う方法の１つとして、信頼の高い第三者による外部認証機関を介した電子情報の授受が知られている。このような従来技術は、例えば特開２００２－１３２１４５号公報などの文献に開示されている。
【0003】
【特許文献1】特開２００２－１３２１４５号公報
【発明の開示】
【発明が解決しようとする課題】
【0004】
ところで、上述した第三者認証機関を利用する電子認証では、より安全性の高い認証を行うことが可能となるが、当事者の双方が事前に認証機関への登録手続きが必要であったり、電子情報のやり取りを行う毎にネットワークを介して認証機関へ接続する必要がある

など、利用者の利便性に欠けると共にコストが高くつくという不都合がある。特に、上述したような受領書や発注書等の授受手続きのように、日常生活に密着した事柄に関する電子認証については、より低コストで簡便に認証手続きを行なえることが望ましい。

【0005】

そこで、本発明は、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことを可能とする電子認証方法及びシステムを提供することを目的とする。

【課題を解決するための手段】

【0006】

第１の態様の本発明は、第１の装置と第２の装置との相互間において、互いが有する平文の同一性を認証する電子認証方法であって、上記第１の装置が、上記平文に対して、可換性を有する暗号方式に基づく第１の暗号鍵を用いた暗号化処理を行って第１の暗号化情報を生成する第１ステップと、上記第２の装置が、上記平文に対して、可換性を有する暗号方式に基づく第２の暗号鍵を用いた暗号化処理を行って第２の暗号化情報を生成する第２ステップと、上記第１の装置が、上記第１の暗号化情報を上記第２の装置に送る第３ステップと、上記第２の装置が、上記第２の暗号化情報を上記第１の装置に送る第４ステップと、上記第１の装置が、上記第２の装置から取得した上記第２の暗号化情報に対して、上記第１の暗号鍵を用いた暗号化処理を行って第３の暗号化情報を生成して自装置内に記憶する第５ステップと、上記第２の装置が、上記第１の装置から取得した上記第１の暗号化情報に対して、上記第２の暗号鍵を用いた暗号化処理を行って第４の暗号化情報を生成して自装置内に記憶する第６ステップと、上記第１の装置が、上記第３の暗号化情報を上記第２の装置に送る第７ステップと、上記第２の装置が、上記第４の暗号化情報を上記第１の装置に送る第８ステップと、上記第１の装置が、自装置内に記憶した上記第３の暗号化情報と上記第２の装置から取得した上記第４の暗号化情報とが一致するか否かを判定し、一致する場合に上記平文の同一性が有効であると認証する第９ステップと、上記第２の装置が、自装置内に記憶した上記第４の暗号化情報と上記第１の装置から受け取った上記第３の暗号化情報とが一致するか否かを判定し、一致する場合に上記平文の同一性が有効であると認証する第１０ステップと、を含むことを特徴とする電子認証方法である。

【0007】

ここで、本明細書において「平文」とは、暗号化処理などの処理がなされていない状態の電子情報（電子データ）をいい、各種の契約書、受領書その他の文書データが含まれる。また「可換性を有する暗号方式」とは、暗号化の対象となる電子情報に対して、少なくとも２回の暗号化処理を行う場合において、当該暗号化処理の１回目に行うものと２回目に行うものとで順番を相互に入れ替えても結果が同じとなるものをいう。

【0008】

かかる方法では、平文に対して、第１の装置及び第２の装置の双方が、可換性を有する暗号方式に基づく暗号鍵を用いて１回目の暗号化を行い、生成された暗号化情報（第１又は第２の暗号化情報）を互いに授受する。次に、第１の装置及び第２の装置の双方が、相手装置から受け取った暗号化情報に対して、可換性を有する暗号方式に基づく暗号鍵を用いて２回目の暗号化を行い、生成された暗号化情報（第３又は第４の暗号化情報）を自装置に記憶すると共に相手装置と授受する。この手順により、双方の装置には、自装置が暗号化してその後に相手装置が暗号化して得られた暗号化情報と、相手装置が暗号化してその後に自装置が暗号化して得られた暗号化情報とが得られる。よって、これらの暗号化情報の一致判定を行うことにより当事者双方の平文の同一性を認証することができる。したがって、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことが可能となる。

【0009】

また、上記第３及び第４ステップにおいて、上記第１及び第２の装置のそれぞれは、上記第１及び第２の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが好ましい。

【0010】
また、上記第７及び第８ステップにおいて、上記第１及び第２の装置のそれぞれは、上記第３及び第４の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが好ましい。
【0011】
また、上記第１及び第２の暗号鍵は、上記第１乃至第１０ステップによる一連の認証処理を行う都度に異なる使い捨て鍵であることが好ましい。
【0012】
第２の態様の本発明は、第１の装置と第２の装置との相互間において、互いが有する平文の同一性を認証する電子認証システムであって、上記第１及び第２の装置のそれぞれは暗号化手段、通信手段、記憶手段及び認証手段を備え、当該第１及び第２の装置が以下のように動作することを特徴とする電子認証システムである。すなわち、
（１）上記第１の装置は、上記暗号化手段により、上記平文に対して、可換性を有する暗号方式に基づく第１の暗号鍵を用いた暗号化処理を行って第１の暗号化情報を生成し、当該第１の暗号化情報を上記通信手段により上記第２の装置に送る。
（２）上記第２の装置は、上記暗号化手段により、上記平文に対して、可換性を有する暗号方式に基づく第２の暗号鍵を用いた暗号化処理を行って第２の暗号化情報を生成し、当該第２の暗号化情報を上記通信手段により上記第１の装置に送る。
（３）上記第１の装置は、上記第２の装置から取得した上記第２の暗号化情報に対して、上記暗号化手段により上記第１の暗号鍵を用いた暗号化処理を行って第３の暗号化情報を生成して上記記憶手段に記憶するとともに、当該第３の暗号化情報を上記通信手段により上記第２の装置に送る。
（４）上記第２の装置は、上記第１の装置から取得した上記第１の暗号化情報に対して、上記第２の暗号鍵を用いた暗号化処理を行って第４の暗号化情報を生成して上記記憶手段に記憶するとともに、当該第４の暗号化情報を上記通信手段により上記第１の装置に送る。
（５）上記第１の装置は、上記認証手段により、上記記憶手段に記憶した上記第３の暗号化情報と上記第２の装置から取得した上記第４の暗号化情報とが一致するか否かを判定し、一致する場合に上記平文の同一性が有効であると認証する。
（６）上記第２の装置は、上記認証手段により、上記記憶手段に記憶した上記第４の暗号化情報と上記第１の装置から取得した上記第３の暗号化情報とが一致するか否かを判定し、一致する場合に上記平文の同一性が有効であると認証する。
【0013】
かかるシステムでは、平文に対して、第１の装置及び第２の装置の双方が、可換性を有する暗号方式に基づく暗号鍵を用いて１回目の暗号化を行い、生成された暗号化情報（第１又は第２の暗号化情報）を互いに授受する。次に、第１の装置及び第２の装置の双方が、相手装置から受け取った暗号化情報に対して、可換性を有する暗号方式に基づく暗号鍵を用いて２回目の暗号化を行い、生成された暗号化情報（第３又は第４の暗号化情報）を自装置に記憶すると共に相手装置と授受する。これにより、双方の装置には、自装置が暗号化してその後に相手装置が暗号化して得られた暗号化情報と、相手装置が暗号化してその後に自装置が暗号化して得られた暗号化情報とが得られる。よって、これらの暗号化情報の一致判定を行うことにより当事者双方の平文の同一性を認証することができる。したがって、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことが可能となる。
【0014】
また、上記第１の装置の上記通信手段と上記第２の装置の上記通信手段は、それぞれ上記第１及び第２の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが好ましい。
【0015】
また、上記第１の装置の上記通信手段と上記第２の装置の上記通信手段は、それぞれ上

記第３及び第４の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが好ましい。

【0016】

また、上記第１及び第２の暗号鍵は、認証処理を行う都度に異なる使い捨て鍵であることが好ましい。

【発明の効果】

【0017】

本発明によれば、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことが可能となる。

【発明を実施するための最良の形態】

【0018】

以下、本発明の実施の形態について図面を参照しながら説明する。

【0019】

始めに本実施形態において使用される「可換性のある暗号方式」について説明する。一例として離散対数問題を利用する方法について説明する。

【0020】

認証対象となる平文をＴとし、この平文ＴをＡとＢの二者間（二装置間）で認証する場合を考える。一方のＡが有する平文Ｔを以後「Ｔａ」と表記し、他方のＢが有する平文Ｔを以後「Ｔｂ」と表記する。

【0021】

まず、大きな素数Ｐを選ぶ。Ｐはシステムに共通とする。

【0022】

今、Ａは鍵X_A（$0 \leqq X_A < P-1$）を生成し、下記計算を行う。

【0023】

【数1】

$$y_A \equiv Ta^{X_A} \bmod P$$

【0024】

y_AからX_Aを求めるのは離散対数計算の困難さから難しいので、Ｔａからy_Aを生成できるのはX_Aを知っているＡだけである。Ａはこの計算結果y_AをＢに送る。

【0025】

Ｂは鍵X_B（$0 \leqq X_B < P-1$）を生成し、下記計算を行う。

【0026】

【数2】

$$y_B \equiv Tb^{X_B} \bmod P$$

【0027】

上記と同様に、y_BからX_Bを求めるのは離散対数計算の困難さから難しいので、Ｔｂからy_Bを生成できるのはX_Bを知っているＢだけである。Ｂはこの計算結果y_BをＡに送る。

【0028】

Ａはy_Bに対して、自らの鍵X_Aを用いて、下記ｙを計算する。

【0029】

【数3】

$$y = y_B^{X_A} = Tb^{X_B \cdot X_A} \bmod P$$

【0030】

Ｂはy_Aに対して、自らの鍵X_Bを用いて、下記ｙを計算する。

【0031】

【数4】

$$y = y_A^{X_B} = Ta^{X_A \cdot X_B} \bmod P$$

【0032】

このとき、Ａが求めたｙとＢが求めたｙとが等しければ、下記の式が成り立ち、Ｔａ＝Ｔｂが証明される。

【0033】

【数5】

$$y = Tb^{X_B \cdot X_A} = Tb^{X_A \cdot X_B} = Ta^{X_A \cdot X_B} \bmod P$$

【0034】

従来のデジタル署名では、公開鍵暗号であるＲＳＡ暗号を用いて上記と同様な効果を有する証明を行っていた。これに対して、本実施形態では、公開鍵を利用せず、当事者間だけで文書の一致を検証することに特徴がある。ただし、上記素数Ｐについては、当事者の相互間で同じ値を使用する必要がある。電子印鑑等の認証装置に本実施形態の認証方式を採用する場合であれば、例えば当該電子印鑑等の製造者が素数Ｐを定める。

【0035】

本実施形態では、以上に説明したような可換性を有する暗号方式を利用して、二者間のみで信頼性の高い認証を可能としている。以下、かかる暗号方式を採用したシステムの実施の形態について更に詳細に説明する。

【0036】

図１は、本発明を適用した一実施形態の電子認証システムの構成を説明する図である。図１に示す電子認証システムは、通信媒体３を介して相互に接続された第１の装置１と第２の装置２とを含んで構成される。本システムでは、第１及び第２の装置の相互間において、互いが有する平文の同一性についての認証が行われる。

【0037】

第１の装置１は、当該装置の全体動作を制御する制御部１０と、外部装置との情報通信処理を担う通信処理部（通信手段）１４と、各種の操作指示を入力するために用いられる操作部１５と、第１の装置１の動作状態等を表示するための表示部１６と、外部メモリ等との間での情報の授受を行うための入出力インタフェース（Ｉ／Ｆ）１７と、を含んで構成される。

【0038】

制御部１０は、例えばＣＰＵ、ＲＯＭ、ＲＡＭなどを含んで構成されるいわゆるコンピュータと、当該コンピュータに所定の処理を行わせ、或いは所定の処理を実現する手段として機能させるためのプログラムとが協働して実現される。この制御部１０は、暗号化処理部１１、記憶部１２、認証処理部１３を含む。

【0039】

暗号化処理部（暗号化手段）１１は、上述した平文或いはその他の電子情報に対して、所定の暗号方式による暗号化を行うものである。特に本実施形態では、この暗号化処理部１１において用いる暗号方式として、可換性を有する暗号方式を採用している。

【0040】

記憶部（記憶手段）１２は、上述した平文或いはその他の電子情報を記憶するものである。

【0041】

認証処理部（認証手段）１３は、自装置（第１の装置１）が有する平文と、相手側装置（第２の装置２）の有する平文とが同一なものであるか否か、すなわち平文の同一性につ

いての認証を行うものである。

【0042】

第２の装置２は、当該装置の全体動作を制御する制御部２０と、外部装置との情報通信処理を担う通信処理部（通信手段）２４と、各種の操作指示を入力するために用いられる操作部２５と、第２の装置２動作状態等を表示するための表示部２６と、外部メモリ等との間での情報の授受を行うための入出力インタフェース（Ｉ／Ｆ）２７と、を含んで構成される。また制御部２０は、暗号化処理部（暗号化手段）２１、記憶部（記憶手段）２２、認証処理部（認証手段）２３を含む。この第２の装置２の構成は上述した第１の装置と同様であるので、各構成要素についての詳細な説明は省略する。

【0043】

本実施形態の電子認証システムはこのような構成を有しており、次に認証処理の詳細について説明する。

【0044】

図２は、本実施形態の電子認証システムにおける認証処理の手順を説明するフローチャートである。本フローチャートでは、第１の装置１と第２の装置２のそれぞれの動作内容が並行して示されている。

【0045】

まず、第１の装置１と第２の装置２とが同一の平文Ｔを取得する（ステップＳ１００、Ｓ２００）。各装置における平文の取得は、例えば入出力Ｉ／Ｆ１７、２７のそれぞれを介して行われる。なお、説明の便宜上、以下では、第１の装置１が取得した平文を「Ｔａ」、第２の装置が取得した平文を「Ｔｂ」とそれぞれ表記する。

【0046】

次に、第１の装置１は、平文Ｔａに対して、可換性を有する暗号方式に基づく第１の暗号鍵Ｋａを用いた暗号化処理を行って第１の暗号化情報（Ｔａ）Ｋａを生成する（ステップＳ１０１）。より具体的には当該処理は暗号化処理部１１によって行われる。

【0047】

また、第２の装置は、平文Ｔｂに対して、可換性を有する暗号方式に基づく第２の暗号鍵Ｋｂを用いた暗号化処理を行って第２の暗号化情報（Ｔｂ）Ｋｂを生成する（ステップＳ２０１）。より具体的には当該処理は暗号化処理部２１によって行われる。

【0048】

ここで、上記第１の暗号鍵Ｋａ及び第２の暗号鍵Ｋｂは、それぞれ一連の認証処理を行う都度に異なる使い捨て鍵であることが望ましい。

【0049】

次に、第１の装置１は、第１の暗号化情報（Ｔａ）Ｋａを第２の装置に送信する（ステップＳ１０２）。より具体的には当該処理は通信処理部１４によって行われる。

【0050】

また、第２の装置２は、第２の暗号化情報（Ｔｂ）Ｋｂを第１の装置１に送信する（ステップＳ２０２）。より具体的には当該処理は通信処理部２４によって行われる。

【0051】

第１の装置１は、第２の装置から送られた第２の暗号化情報（Ｔｂ）Ｋｂを受信する。（ステップＳ１０３）。より具体的には当該処理は通信処理部１４によって行われる。また、第２の装置２は、第１の装置から送られた第１の暗号化情報（Ｔａ）Ｋａを受信する。（ステップＳ２０３）。より具体的には当該処理は通信処理部２４によって行われる。

【0052】

ここで、第１及び第２の暗号化情報の送信及び受信は、当該第１及び第２の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが望ましい。例えば、本実施形態では、第１の装置１と第２の装置２との間で、互いに１ビットずつ交互にデータを送り合うようにする。これにより、仮に第１及び第２の暗号化情報の送信／受信時にこれらの暗号化情報を来た方向に折り返す不正操作を回避することが可能となる。なお、部分情報のデータ量は１ビットずつに限定されるものではなく、任意に変更可能である。

【0053】
次に、第１の装置１は、第２の装置２から取得した第２の暗号化情報（Ｔｂ）ＫｂＫａに対して、第１の暗号鍵Ｋａを用いた暗号化処理を行って第３の暗号化情報（Ｔｂ）ＫｂＫａを生成して自装置内に記憶する（ステップＳ１０４）。より具体的には、第３の暗号化情報の生成は暗号化処理部１１により行われ、当該第３の暗号化情報の記憶は記憶部１２により行われる。
【0054】
また、第２の装置２は、第１の装置１から取得した第１の暗号化情報（Ｔａ）Ｋａに対して、第２の暗号鍵Ｋｂを用いた暗号化処理を行って第４の暗号化情報（Ｔａ）ＫａＫｂを生成して自装置内に記憶する（ステップＳ２０４）。より具体的には、第４の暗号化情報の生成は暗号化処理部２１により行われ、当該第４の暗号化情報の記憶は記憶部２２により行われる。
【0055】
次に、第１の装置１は、第３の暗号化情報（Ｔｂ）ＫｂＫａを第２の装置２に送信する（ステップＳ１０５）。より具体的には当該処理は通信処理部１４によって行われる。
【0056】
また、第２の装置２は、第４の暗号化情報（Ｔａ）ＫａＫｂを第１の装置１に送信する（ステップＳ２０５）。より具体的には当該処理は通信処理部２４によって行われる。
【0057】
第１の装置１は、第２の装置から送られた第４の暗号化情報（Ｔａ）ＫａＫｂを受信する。（ステップＳ１０６）。より具体的には当該処理は通信処理部１４によって行われる。また、第２の装置２は、第１の装置から送られた第３の暗号化情報（Ｔｂ）ＫｂＫａを受信する。（ステップＳ２０６）。より具体的には当該処理は通信処理部２４によって行われる。
【0058】
ここで、第３及び第４の暗号化情報の送信及び受信は、当該第３及び第４の暗号化情報を複数の部分情報に分割して当該部分情報を交互に送信し合うことが望ましい。例えば、本実施形態では、第１の装置１と第２の装置２との間で、互いに１ビットずつ交互にデータを送り合うようにする。これにより、仮に第３及び第４の暗号化情報の送信／受信時にこれらの暗号化情報を来た方向に折り返す不正操作を回避することが可能となる。なお、部分情報のデータ量は１ビットずつに限定されるものではなく、任意に変更可能である。
【0059】
次に、第１の装置１は、自装置内に記憶した第３の暗号化情報（Ｔｂ）ＫｂＫａと第２の装置２から取得した第４の暗号化情報（Ｔａ）ＫａＫｂとが一致するか否かを判定する（ステップＳ１０７）。より具体的には、当該判定は認証処理部１３によって行われる。可換性を有する暗号方式を採用しているので、第１の装置１が有する平文Ｔａと第２の装置２が有する平文Ｔｂのいずれか或いは両方が、何らかの方法で改ざん、偽造等されていなければ、（Ｔｂ）ＫｂＫａ＝（Ｔａ）ＫａＫｂとなる。よって、第３及び第４の暗号化情報の一致判断を行えば、平文の同一性について認証できる。
【0060】
第３の暗号化情報と第４の暗号化情報とが一致する場合には、ステップＳ１０７で肯定判断（ＹＥＳ）がなされ、第１の装置１は、平文が同一、すなわち平文の同一性が有効であると認証する（ステップＳ１０８）。より具体的には当該認証は認証処理部１３により行われる。
【0061】
また、第３の暗号化情報と第４の暗号化情報とが一致しない場合には、ステップＳ１０７で否定判断（ＮＯ）がなされ、第１の装置１は、平文の同一性が有効ではないと認証して一連の処理を終了する。
【0062】
なお、平文の同一性についての認証結果は、例えば表示部１６を介して使用者に提示さ

れ、或いは相手側である第２の装置２に通知される。

【0063】

また、第２の装置２は、自装置内に記憶した第４の暗号化情報（Ｔａ）ＫａＫｂと第１の装置１から取得した第３の暗号化情報（Ｔｂ）ＫｂＫａとが一致するか否かを判定する（ステップＳ２０７）。より具体的には、当該判定は認証処理部２３によって行われる。可換性を有する暗号方式を採用しているので、第１の装置１が有する平文Ｔａと第２の装置２が有する平文Ｔｂのいずれか或いは両方が、何らかの方法で改変、偽造等されていなければ、（Ｔａ）ＫａＫｂ＝（Ｔｂ）ＫｂＫａとなる。よって、第３及び第４の暗号化情報の一致判断を行えば、平文の同一性について認証できる。

【0064】

第４の暗号化情報と第３の暗号化情報とが一致する場合には、ステップＳ２０７で肯定判断（ＹＥＳ）がなされ、第２の装置２は、平文が同一、すなわち平文の同一性が有効であると認証する（ステップＳ２０８）。より具体的には当該認証は認証処理部２３におり行われる。

【0065】

また、第４の暗号化情報と第３の暗号化情報とが一致しない場合には、ステップＳ２０７で否定判断（ＮＯ）がなされ、第２の装置２は、平文の同一性が有効ではないと認証して一連の処理を終了する。

【0066】

なお、平文の同一性についての認証結果は、例えば表示部２６を介して使用者に提示され、或いは相手側である第１の装置１に通知される。

【0067】

このように、本実施形態では、平文に対して当事者双方の装置がまず１回目の暗号化を行って生成した暗号化情報を互いに授受し、次に相手装置から受け取った暗号化情報に対して更に２回目の暗号化を行って生成した暗号化情報を自装置に記憶すると共に相手装置と授受する。この２回の暗号化がなされることにより、双方の装置には、（１）まず自装置が暗号化し、その後相手装置が暗号化して得られた暗号化情報と、（２）まず相手装置が暗号化し、その後自装置が暗号化して得られた暗号化情報とが得られる。可換性を有する暗号方式を採用していることから、上記（１）、（２）の暗号化情報は、原理的に一致するので、当該暗号化情報についての一致判定を行うことにより、当事者双方が有する平文の同一性を認証することができる。したがって、第三者機関を介さずに、当事者間で電子情報の相互認証の手続きを低コストかつ簡便に行うことが可能となる。

【0068】

次に、上述した電子認証システムの応用例と当該システムに用いられる電子印鑑（電子認証装置）についての具体例を説明する。

【0069】

図３は、電子印鑑の具体例について説明する図（斜視図）である。本例の電子印鑑は、例えばＰＣＭＣＩＡカードに準拠した入出力インタフェースを有するカード状の電子印鑑であり、その内部に上述した実施形態にかかる第１の装置１又は第２の装置２と同等の構成を備えている。

【0070】

図３に示す電子印鑑１００は、操作キー（数字キー）１０１、ランプ１０２～１０５、カメラユニット１０６、液晶表示部１０７、入出力インタフェース１０８を含んで構成されている。

【0071】

操作キー１０１は、例えば１～９の数字キー等を含むものであり、操作指示の入力に用いられる。当該操作キー１０１は、上述した操作部１５又は２５に対応するものである。

【0072】

ランプ１０２～１０５は、電子印鑑の動作状態、より詳細には認証結果に関する表示を行うためのものである。各ランプの点灯状態を認証結果との対応の詳細については後述す

る。なお、これらのランプ１０２～１０５と液晶表示部１０７とが、上述した表示部１６又は２６に対応している。

【0073】

カメラユニット１０６は、電子印鑑１００を用いる使用者を撮像し、画像データを得るためのものである。カメラユニット１０６による撮像タイミングや得られた画像データの用途等の詳細については後述する。

【0074】

液晶表示部１０７は、電子印鑑の動作状態について、ランプ１０２等により表現し切れない詳細な情報を使用者に伝えるための文字や画像等を表示するものである。

【0075】

入出力インタフェース１０８は、ＰＣＭＣＩＡカードの規格に準拠したものであり、例えばパーソナルコンピュータ等の外部機器と電子印鑑１００とを接続し、データ通信を行うためのものである。

【0076】

本例の電子印鑑１００はこのような構成を備えると共に、上述した第１又は第２の装置に相当する機能を備えており、次に当該電子印鑑１００を使用した電子認証手続きの例について説明する。以下では、例えば消費者Ａが宅配業者Ｂから配送品を受け取る際に、受け取りの確認を行う文書である受領書を電子情報（平文）により用意し、当該受領書に対して両当事者Ａ，Ｂが互いに電子印鑑を用いて押印する場合を想定して説明する。

【0077】

ここで、以降の説明に用いるいくつかの記号、略号について定義する。

(1)Ａ，Ｂ：それぞれ消費者と宅配業者である。

(2)電子印鑑１００Ａ：消費者Ａが使用する電子印鑑である。

(3)電子印鑑１００Ｂ：宅配業者Ｂが使用する電子印鑑である。

(4)Ｔ：Ａ，Ｂが合意した内容を含み、認証の対象となる文書（平文）であり本例では受領書である。押印が終わったあとに電子印鑑１００Ａ及び１００Ｂに同じものが保存される。

(5)Ｔｆ：正規の平文Ｔに代わるべく悪意の他者（Ａ又はＢも当該他者となり得る）が改ざんした平文である。

(6)スタンプＩＤ：各電子印鑑に固有の識別番号であり、電子印鑑の製造時に設定される不変の番号である。電子印鑑１００Ａのスタンプ ＩＤを「ＩＤＡ」、電子印鑑１００Ｂのスタンプ ＩＤを「ＩＤＢ」とする。

(7)ＩｎｃｒＮ：使用履歴に応じて変化する番号であり、予め設定された規則（ロジック）により変化する。電子印鑑１００Ａの番号を「ＩｎｃｒＮＡ」、電子印鑑１００Ｂの番号を「ＩｎｃｒＮＢ」とする。このＩｎｃｒＮは、メーカにより特定の変化をするように設定される数であり、同じ数は２度と現れない。メーカは、依頼があればその電子印鑑が発生し得るＩｎｃｒＮであるか否かを明らかにできる。

(8)Ｉｎｃｒ：ＩｎｃｒＮを暗号化して変化のロジックを見えなくしたものである。電子印鑑１００Ａの番号を「ＩｎｃｒＡ」、電子印鑑１００Ｂの番号を「ＩｎｃｒＢ」とする。本例では、所定の暗号鍵（後述する）により暗号化した数をＩｎｃｒとする。

(9)ＴＩＤ：記録されている自分と相手のそれぞれのスタンプＩＤ及びＩｎｃｒの計４つによって特定される情報であり、システム内で一意である。

(10)ＴＩＤＡ：ＩＤＡとＩｎｃｒＡとの組み合わせである。電子印鑑１００Ａ内で一意である。

(11)ＴＩＤＢ：ＩＤＢとＩｎｃｒＢとの組み合わせである。電子印鑑１００Ｂ内で一意である。

(12)Ｔｅｘｔ：当事者Ａ，Ｂが合意した内容である。

(13)Ｔｅｘｔｆ：当事者の一方がＴｅｘｔの内容を改ざんしたものである。

(14)Ｔａ：当事者Ａが正しい（有効）として電子印鑑１００Ａ内に記録し、認証に使う文書である。

(15)Ｔｂ：当事者Ｂが正しい（有効）として電子印鑑１００Ｂ内に記録し、認証に使う文書である。
(16)Ｋｔ：電子印鑑のメーカ（製造者）と通信するときに使用する暗号鍵である。鍵毎に固有で不変であり、メーカが生成して各電子印鑑に設定する。電子印鑑１００Ａの鍵を「Ｋｔａ」、電子印鑑１００Ｂの鍵を「Ｋｔｂ」とする。
(17)Ｋｉｎｃｒ：上述したＩｎｃｒを暗号化するための鍵であり、電子印鑑の使用に先立って、印鑑内部の乱数発生装置によって生成される。誰にも知られることがないものである。電子印鑑１００Ａの鍵を「ＫｉｎｃｒＡ」、電子印鑑１００Ｂの鍵を「ＫｉｎｃｒＢ」とする。
(18)Ｋ：認証時に、認証内容を暗号化して交換する際に用いる鍵であり、一回限りの使い捨ての鍵である。電子印鑑１００Ａの鍵を「Ｋａ」、電子印鑑１００Ｂの鍵を「Ｋｂ」とする。
(19)ランプＬｓ：押印時に正しい文書を電子印鑑の相互間で共有できたか否かを表示するためのランプである。電子印鑑１００Ａのランプを「ＬｓＡ」、電子印鑑１００Ｂのランプを「ＬｓＢ」とする。上述したランプ１０２～１０５のいずれかがランプＬｓに対応する。
(20)ランプＬｉ：認証時に、電子印鑑の所有者が正しいと主張する文書が本当に正しいか否かを表示するためのランプである。電子印鑑１００Ａのランプを「ＬｉＡ」、電子印鑑１００Ｂのランプを「ＬｉＢ」とする。上述したランプ１０２～１０５のいずれかがランプＬｉに対応する。
(21)ランプＬｊ：認証時に、相手が正しいと主張する文書がＴと一致するか否かを表示するためのランプである。電子印鑑１００Ａのランプを「ＬｊＡ」、電子印鑑１００Ｂのランプを「ＬｊＢ」とする。上述したランプ１０２～１０５のいずれかがランプＬｊに対応する。
(22)ランプＬｆ：認証時、現在送っている文書がＴであるか、ＴａあるいはＴｂなのかを表示するためのランプである。このランプの点灯状態は上述したカメラユニット１０６にも写り込む。電子印鑑１００Ａのランプを「ＬｆＡ」、電子印鑑１００Ｂの鍵を「ＬｆＢ」とする。上述したランプ１０２～１０５のいずれかがランプＬｆに対応する。
(23)Ｈｕｓｈ：テキスト、スタンプＩＤ、Ｉｎｃｒ、画像データに対する改ざん防止符号である。
(24)Ｖ：カメラユニット１０６により撮像され、押印相手の電子印鑑へ送られている動画像である。電子印鑑を使用する者の顔などが含まれる。電子印鑑１００Ａが相手方に送っている動画像をＶａ、電子印鑑１００Ｂが相手方に送っている動画像をＶｂとする。
(25)Ｖｉ：上記Ｖを所定のタイミング（後述する）で固定した静止画像である。スタンプＩＤとＩｎｃｒＮとが合成されている。電子印鑑１００Ａが相手方に送る静止画像をＶｉａとする。このＶｉａにより、相手方の電子印鑑１００Ｂの使用者の顔等と、スタンプＩＤ（ＩＤＢ）、ＩｎｃｒＮ（ＩｎｃｒＮＢ）とが目視できる。電子印鑑１００Ｂが相手方に送る静止画像をＶｉｂとする。このＶｉｂにより、相手方の電子印鑑１００Ａの使用者の顔等と、スタンプＩＤ（ＩＤＡ）、ＩｎｃｒＮ（ＩｎｃｒＮＡ）とが目視できる。

【0078】

図４は、当事者のいずれも改ざん等の不正を行わない正常な状況における電子印鑑の使用時の構成例を示す図である。端末装置１１０Ａは当事者Ａの電子印鑑１００Ａを接続するための装置、端末装置１１０Ｂは当事者Ｂの電子印鑑１００Ｂを接続するための装置であり、これらの端末装置間が所定の通信路１２０により相互に接続される。本実施形態では、図中で一点鎖線により示すように、これらの端末装置１１０Ａ、１１０Ｂ及び通信路１２０の機能を備え、電子印鑑の押印に用いられる押印ユニット（伝送装置）を用いる。以下に押印手順を説明する。

【0079】

まず、電子印鑑１００Ａと電子印鑑１００Ｂとの相互間で、スタンプＩＤを交換する。

【0080】

次に、合意した契約文書Ｔを用意し、各端末装置１００Ａ、１００Ｂを介して電子印鑑１００Ａと電子印鑑１００Ｂの双方に送り、記録させる。電子印鑑１００Ａ内にＴａが記録され、電子印鑑１００Ｂ内にＴｂが記録される。

【0081】

次に、押印状況を示す動画像Ｖがカメラユニット１０６により撮像され、相手側の電子印鑑へ送られる。静止画像Ｖｉの撮像タイミングについては相手が決定し、電子印鑑を用いて当該タイミングを指示する。

【0082】

例えば、電子印鑑１００Ａで撮像された動画像Ｖａは電子印鑑１００Ｂへ送られ、電子印鑑１００Ｂに備わった液晶表示部１０７に表示される。当該表示を見ながら、電子印鑑１００Ｂを使用する当事者Ｂにより操作部１０１を用いて適当なタイミングが指示されると、当該指示が電子印鑑１００Ａに送られる。このタイミングで電子印鑑１００Ａは静止画像Ｖｉａを生成する。この静止画像Ｖｉａには電子印鑑１００Ａに対応するスタンプＩＤとＩｎｃｒとが合成される。またこのとき、電子印鑑１００Ａは、スタンプＩＤ等を合成する前の静止画像（或いは動画像でもよい）を自装置内に保存する。

【0083】

同様に、電子印鑑１００Ｂで撮像された動画像Ｖｂは電子印鑑１００Ａへ送られ、電子印鑑１００Ａに備わった液晶表示部１０７に表示される。当該表示を見ながら、電子印鑑１００Ａを使用する当事者Ａにより操作部１０１を用いて適当なタイミングが指示されると、当該指示が電子印鑑１００Ｂに送られる。このタイミングで電子印鑑１００Ｂは静止画像Ｖｉａを生成する。この静止画像Ｖｉａには電子印鑑１００Ｂに対応するスタンプＩＤとＩｎｃｒとが合成される。またこのとき、電子印鑑１００Ｂは、スタンプＩＤ等を合成する前の静止画像（或いは動画像でもよい）を自装置内に保存する。

【0084】

次に、電子印鑑１００Ａと電子印鑑１００Ｂは、互いに静止画像を交換し合う。具体的には、電子印鑑１００Ａは静止画像Ｖｉａを電子印鑑１００Ｂに送り、電子印鑑１００Ｂは静止画像Ｖｉｂを電子印鑑１００Ａに送る。

【0085】

次に、電子印鑑１００Ａを使用する当事者Ａにより、液晶表示部１０７に表示された静止画像Ｖｉｂに含まれるＩｎｃｒＢが参照され、これに対応する数値が操作部１０１を用いて入力されると、電子印鑑１００Ａはこの入力された数値を電子印鑑１００Ｂに送る。並行して、電子印鑑１００Ｂを使用する当事者Ｂにより、液晶表示部１０７に表示された静止画像Ｖｉａに含まれるＩｎｃｒＡが参照され、これに対応する数値が操作部１０１を用いて入力されると、電子印鑑１００Ｂはこの入力された数値を電子印鑑１００Ａに送る。これらのＩｎｃｒＮに対応する数値の交換は、当事者の両方が入力を完了した後に行われることが望ましい。

【0086】

次に、電子印鑑１００Ａは、電子印鑑１００Ｂから送られてきたＩｎｃｒＢと、当事者Ａにより画像を参照して手入力された上記数値とを比較して一致を確認する。一致が確認されない場合には、例えば、押印処理が無効であるとして中断され、押印処理のやり直しが要求される。

【0087】

同様に、電子印鑑１００Ｂは、電子印鑑１００Ａから送られてきたＩｎｃｒＡと、当事者Ｂにより画像を参照して手入力された上記数値とを比較して一致を確認する。一致が確認されない場合には、例えば、押印処理が無効であるとして中断され、押印処理のやり直しが要求される。

【0088】

各電子印鑑ともに一致判定が得られた場合には以下の処理が継続される。

【0089】

電子印鑑１００Ａは、Ｔａに自己のスタンプＩＤＡ、ＩｎｃｒＡ、Ｖｉｂ、相手のスタ

ンプＩＤＢ、ＩｎｃｒＢを加えて（関連付けて）文書Ｔを生成し、当該Ｔを保存する。

【0090】

同様に、電子印鑑１００Ｂは、Ｔｂに自己のスタンプＩＤＢ、ＩｎｃｒＢ、Ｖｉａ、相手のスタンプＩＤＡ、ＩｎｃｒＡを加えて（関連付けて）文書Ｔを生成し、当該Ｔを保存する。

【0091】

次に、上述した電子認証システムにおいて詳述した方法により、文書Ｔの認証処理がなされる。具体的には、電子印鑑１００Ａは、ＴａをＫａにより暗号化して（Ｔａ）Ｋａを作成し、これを電子印鑑１００Ｂに送る。同様に、電子印鑑１００Ｂは、ＴｂをＫｂにより暗号化して（Ｔｂ）Ｋｂを作成し、これを電子印鑑１００Ａに送る。電子印鑑１００Ａは、（Ｔｂ）ＫｂをＫａにより暗号化して（Ｔｂ）ＫｂＫａを作成し、これを保存するとともに電子印鑑１００Ｂに送る。また、電子印鑑１００Ｂは、（Ｔａ）ＫａをＫｂにより暗号化して（Ｔａ）ＫａＫｂを作成し、これを保存するとともに電子印鑑１００Ａに送る。本実施形態で使用する暗号化方式は暗号化の順序を変えても結果が同じとなる性質（可換性）をもつから、Ｔａ＝Ｔｂであれば（Ｔａ）ＫａＫｂ＝（Ｔｂ）ＫｂＫａとなるし、その逆もまた真となる性質（一意性）をもつ。各電子印鑑は、暗号化して送られたきた値と自装置に保存してある値とを比較することで、相手が同じＴｅｘｔを電子印鑑の内部に保存しているか否かを検証できる。

【0092】

また、こうした一連の認証動作についての履歴情報は、各電子印鑑に蓄積される。例えば、認証動作を行った日時、相手に関する情報（スタンプＩＤ、Ｉｎｃｒ、Ｖｉ等）などが履歴情報として蓄積される。

【0093】

次に、当事者のいずれか（或いは双方とも）により不正な手続きがなされた場合における検証方法について説明する。

【0094】

図５は、当事者のいずれか（或いは双方とも）が改ざん等の不正を行う状況における電子印鑑の使用時の構成例を示す図である。図示のように、電子印鑑１００Ａと端末装置１１０Ａとの間又は電子印鑑１００Ｂと端末装置１１０Ｂとの間に、改ざん装置（フィルター）１３０Ａ又は改ざん装置（フィルター）１３０Ｂが挿入され、不正な手続きがなされる場合を考える。

【0095】

例えば本例では、以下のような前提のもとにシステム運営を行う。

(1)電子印鑑は所定の機能を完全に持っており、故障のことは別に考える。

(2)耐タンパー性、ロバストネスは保証されている。

(3)電子印鑑を使用した人物（Ａ，Ｂ）の特定が画像により可能である。

(4)電子印鑑を紛失した場合は、存在する電子印鑑の判定を正しいとする。

(5)押印済み文書は平文で、どこにでも流布される。

(6)認証・調停を外部に求めない。

(7)押印途中で電子印鑑を伝送装置から外すことは許されない。

(8)電子印鑑は２つの文書を並行して押印することができない。

(9)非対面での押印が可能である。押印は電子印鑑内に保存された文書が一致したことで完了する。

(10)Ａには改ざんの意志が無く、Ｂはあらゆる手投を使って改ざんを行う。どちらがＡでどちらがＢか不定とする。

(11)電子印鑑を特定するためのスタンプＩＤは、メーカ（製造者）により一意に設定されて変化することがない。

(12)押印・認証プロトコルをリードするのはいずれの電子印鑑でも良い。

(13)電子印鑑の使用履歴を表すＩｎｃｒＮは、製造者により特定の変化をするように設定される数で、同じ数は２度と現れない。製造者は依頼があれば特定の電子印鑑が発生し得

ＩｎｃｒＮかどうか明らかにできる。押印／認証時に使用する暗号鍵Ｋは１シーケンスごとに異なる使い捨ての鍵である。
(14)各電子印鑑には点灯により内部状態を表示する５つのランプがある。使用者はこのランプを目視することにより電子印鑑の動作内容を直接知ることが可能である。
【0096】
例えば、攻撃として電子印鑑１００Ｂに有利となる改ざん装置１３０Ｂが使用されている場合を想定する。この改ざん装置１３０Ｂは電子印鑑間の電文を全て記録し、場合に応じて電文を改ざんし、或いはなりすましができる。改ざん装置１３０Ｂの存在がなければ、電子印鑑同士は必ず同一の文書を保存し、保存文書による認証結果が異なることはない。電子印鑑１００Ａの判定と電子印鑑１００Ｂの判定が食い違ったとき、お互いが正（有効）であると主張する文書を、お互いに読み込んで判定させる手順が必要である。
【0097】
各電子印鑑のスタンプＩＤとＩｎｃｒとのは本システムの中で一意に保たれる。電子印鑑内で、同一のＴＩＤ（ＩＤＡ＋ＩｎｃｒＡ＋ＩＤＢ＋ＩｎｃｒＢ）が打たれていて、電子印鑑内に保存されている文書はただ１つである。物理的には２つの電子印鑑にそれぞれ１つずつ保存される。
【0098】
改ざん装置１３０Ｂが、ＩｎｃｒＢとして勝手な値を設定して電子印鑑１００Ａに送ったとしても、電子印鑑１００Ａから正規の電子印鑑１００Ｂに問い合わせがあれば、電子印鑑１００Ｂが出力したことのないＩｎｃｒＢであると否定されることになる。また、メーカに改ざん装置１３０Ｂが作成したＩｎｃｒＢを送れば。真の電子印鑑１００Ｂで作成された値でないことを検証できる。一方、ＩｎｃｒＡは電子印鑑Ａで作られた値であるからメーカで正しいと判定される。
【0099】
次に、電子印鑑Ｂを使わないなりすましがなされた場合を考える。改ざん装置１３０Ｂが電子印鑑１００Ｂになりすまして電子印鑑１００Ａとの押印を試みるとき、改ざん装置１３０ＢはＩｎｃｒＢとして電子印鑑１００Ｂから出力される可能性のある値を使わなければならない。しかし、ＩｎｃｒＢを正常な値に設定できる可能性は低い。ＩｎｃｒＢを正しい値とするためには、電子印鑑Ｂを利用するか、あるいはＩｎｃｒＢを過去の文書から探して利用（盗用）することでメーカを信じさせることができ、電子印鑑ＡにＩｎｃｒＢを使って押印することができる。しかし、正規の電子印鑑１００Ｂには、ＩｎｃｒＢに基づく過去の押印の事実（履歴）が残っているので、電子印鑑１００Ａとの間における押印事実を否定することは可能である。この場合、本例では内容については電子印鑑１００Ａの所有者である当事者Ａの言い分が正しいとされる。内容について電子印鑑１００Ｂの所有者側が反論したい場合には、改ざん装置１３０Ｂは電子印鑑１００ＢにＴｆを記録させる必要がある。
【0100】
当事者Ｂは、当事者Ａが勝手に作成した文書であると反論できるが、反論するために当事者ＢはＩｎｃｒＢは他の電子印鑑との間で使用したものであること、或いは電子印鑑１００Ｂが出力するはずのないものであることを証明する必要がある。２つの証明方法のいずれにも電子印鑑１００Ｂが必要であるので、電子印鑑１００Ｂを使わないなりすましは不可能となる。
【0101】
このように、電子印鑑１００Ｂを使わないなりすましは無意味なので、電子印鑑１００Ｂを使ったなりすましがなされる場合について次に説明する。改ざん装置１３０Ｂが、Ｔｅｘｔに変えてＴｅｘｔｆを電子印鑑１００Ｂに送り込むことは、押印時の検証結果を正（有効）とすることができないので無意味である。電子印鑑１００Ａと電子印鑑１００Ｂとは、改ざん装置１３０Ｂを挟んで押印するとき、ＩｎｃｒＡ、ＩｎｃｒＢとしてそれぞれ自装置の発行したＩｎｃｒを使うことができる。しかし、内容を両電子印鑑そろってＴｅｘｔｆとすることができない。そこで、改ざん装置１３０Ｂは、電子印鑑１００Ａに対

しては電子印鑑１００Ｂであり、電子印鑑１００Ｂに対しては電子印鑑１００Ａであるかのように振る舞い（動作し）、電子印鑑１００Ａに対してはＴを、電子印鑑１００Ｂに対してはＴｆをそれぞれ正当な文書として認証させようと試みる。このような動作は改ざん装置が勝手にＫａ、Ｋｂを設定することでそれぞれ押印時のＴの一致検証を通り抜けられるので可能である。

【0102】

次に、画像の役割を説明する。画像Ｖａは当事者Ｂがその撮像タイミングを指定するので、当事者Ａが押印したという事実を当事者Ｂに認めさせるために使われる（押印相手の確認）。当事者Ｂが指示した動作に当事者Ａが反応すれば、当事者Ｂは当事者Ａを相手に押印しようとしていることを確認できる。同時に当事者ＡはＶａを含むＴに押印すれば、Ｖａが当事者Ａの立体的な肖像を写し取ったものであることを当事者Ａが認めたということになる。同様に画像内に、インサートされたＴＩＤ、文書のタイトルあるいは重要な一部、電子印鑑のおかれた状況（周辺の様子）などが含まれていれば、当事者Ａ、Ｂいずれもこれらを認めたとする。画像Ｖｂも当事者Ａ、Ｂに対する意味あいは同じである。改ざん装置１３０Ｂは過去の記録から現在の画像Ｖａ、Ｖｂを作成することができない。したがって改ざん装置１３０Ｂが電子印鑑Ｂになりすますには電子印鑑１００Ｂと同じ動作をしなければならない。このときＩｎｃｒＢについては、電子印鑑１００Ｂから予めもらわないと後の認証時になりすましであることがわかってしまう。しかし電子印鑑１００ＢからＩｎｃｒＢをもらうと、ＩｎｃｒＢには電子印鑑１００Ａとは違った過去のＶａを使っている。一方、電子印鑑１００ＡにはＶａ、Ｖｂとも疑いの無い映像が記録されている。当事者Ｂはこれ以降、このＴＩＤに対し電子印鑑１００Ｂでは無く改ざん装置１３０Ｂを用いて認証に臨むこととなる。しかるに改ざん装置１３０Ｂは電子印鑑１００Ａとの間でＴの確認をすませているので、Ｔの中のＴｅｘｔを改ざんするしかできない。押印事実そのものの破棄は可能であるが当事者Ｂにとって不利である。また電子印鑑１００Ａはインサート前の画像Ｖａを記録しておくので、Ｖｉａが電子印鑑１００ＡでＶａによって撮影されたことを明瞭に示すことができる。Ｖａは電子印鑑１００Ａにしか知り得ない情報であるためである。画像交換にはＶｉａ、Ｖｉｂに含まれるＴＩＤ（ＩＤＡ、ＩｎｃｒＡ、ＩＤＢ、ＩｎｃｒＢ）がＴに含まれるＴＩＤと一致していると両押印者に確認させる役割がある。

【0103】

電子印鑑１００Ｂ内と異なり、改ざん装置１３０Ｂ内は自由に改ざんをできるので、ＴをＴｆに改ざんしたとすると、電子印鑑１００Ａの保存するＴと矛盾することになる。どちらが正しいかはわからない。この不一致は改ざん装置１３０Ｂの入っている環境では、押印時にはわからず、認証時に判定される。

【0104】

以下、説明を簡単にするため当事者ＢがＴｆを作成し、これが正しい押印文書であると主張した場合を説明する。なお、当事者ＡとＢが入れ替わっても同じことである。

【0105】

まず、自らが押印したことの証明について説明する（検証１）。Ｖｉａ、Ｖｉｂを示して、自らがＴＩＤＢに電子印鑑１００Ａを使って押印したことを示す。認証はＴＩＤＡを電子印鑑１００Ａ、ＴＩＤＢを電子印鑑１００Ｂに示し、保存されているＴを比較すれば良い。それぞれランプＬｉＡ、ランプＬｉＢが正（有効）を示す点灯状態となる。しかし当事者Ｂは悪意を持つから、改ざん装置１３０ＢによってＴの一部を改ざんして電子印鑑Ｂに送り、ＬｉＢを不正とするかもしれない。

【0106】

次に、自らが押印していないことの証明について説明する（検証２）。当事者Ｂは、新たに作成、あるいは既存の文書を利用して改ざんした文書Ｔｆを作成する。この場合、認証はＴｆを電子印鑑１００Ａ、電子印鑑１００Ｂにそれぞれ保存されているＴと比較すればランプＬｉは不正と表示する。しかし当事者Ｂは悪意を持つから、改ざん装置１３０Ｂを作用させ、Ｔｆに変えてＴを電子印鑑１００Ｂに送り、電子印鑑１００ＢのランプＬＩ

Ｂが正（有効）を示すようにするかもしれない。

【0107】

次に、自らも相手も押印したことの証明について説明する。上述した検証１、２により、ＴについてＬＩＡは正、ＴｆについてＬｉＢが正を示す状態となった。このような状態は改ざん装置１３０Ｂが存在しているので、正しいと主張するほうが相手も確かに押印したということを示す必要がある。自分が押印していないというだけでは不十分である。この改ざん装置１３０Ｂは情報伝送手順と以下の情報、Ｔ、Ｔｆ（ＩＤＡ、ＩＤＢ、ＩｎｃｒＡ、ＩｎｃｒＢ、Ｖａ、Ｖｂ）、Ｈｕｓｈ、（Ｈｕｓｈ）Ｋａ、（Ｈｕｓｈ）Ｋｂ、及び認証時点以前に押印、認証に使われた情報すべてを有している。これらの情報は認証に用いると、改ざん装置１３０Ｂで改ざんされるので使えない。Ｋａ、Ｋｂによる暗号が掛けられている情報は、鍵が使い捨てなので安全である。

【0108】

まず、自己認証、すなわち電子印鑑の内部の情報との一致判定について説明する。当事者Ａ、Ｂは、それぞれ自らが正しいと主張する２つの文書Ｔ、Ｔｆを電子印鑑１００Ａ、電子印鑑１００Ｂにそれぞれに送り、Ｔａ、Ｔｂとして保持する（Ｔａ＝Ｔ、Ｔｂ＝Ｔｆ）。同様に相手が正しいと主張する２つの文書Ｔｆ、Ｔを電子印鑑１００Ａ、電子印鑑１００Ｂにそれぞれに送り、Ｔａｊ、Ｔｂｊとして保持する（Ｔａｊ＝Ｔｆ、Ｔｂｊ＝Ｔ）。

【0109】

電子印鑑１００Ａは、内部に蓄横したデータＴにより、受け取ったデータＴａ、Ｔａｊのどちらに自分が押印したことが有るか検査する。電子印鑑１００Ａはまず Ｔａ、Ｔａｊにそれぞれ含まれているＩＤＡ、ＩｎｃｒＡ、ＩＤＢ、ＩｎｃｒＢを検索キーにして、電子印鑑の内部の文書に一致するか検査する。電子印鑑１００Ｂも同じ動作を行う。このとき両者が自らの文書が正しいと主張する以上、Ｔａ＝Ｔ、Ｔｂｊ＝Ｔとなり、ランプＬｉＡと電子印鑑１００ＢのランプＬｉＢが正の表示をするはずである。さらに、ＬｊＡ、ＬｊＢが正の表示となれはＴ＝Ｔｆであり、これ以上の認証は不要である。読込判定時の解釈を以下の表１に示す。

【0110】

【表1】

ケース	ＬｉＡ	ＬｊＡ	ＬｉＢ	ＬｊＢ	判定
1	○	○	○	○	Ｔ＝Ｔｆと判定
2	○	×	×	○	Ｔａ＝Ｔと判定，Ａが正しいと判定
3	×	○	○	×	Ｔｂ＝Ｔと判定，Ｂが正しいと判定
4	○	×	○	×	不正操作（フィルタ操作ｎ）の可能性あり。認証が必要。
5	○	－	×	－	ケース２以外ではＢ側で不正操作の可能性あり。Ｔが正と判断。
6	×	－	○	－	ケース３以外ではＡ側で不正操作の可能性あり。Ｔｆが正と判断。
7	×	－	×	－	不正操作の可能性あり。Ｔａ，Ｔｆとも不正と判定。
8	×	×	×	×	Ｔａ，Ｔａｊ，Ｔｂ，Ｔｂｊとも押印したことはない。

上記表１では、各状況（ケース１，２，３…）におけるランプＬｉＡ等の点灯状態（点灯が「○」、不点灯が「×」、点灯／不点灯を不問の場合が「－」）と、それらの点灯状

態の組み合わせによる判定結果が示されている。例えば、各ランプの点灯状態がケース１に示す状態である場合には、Ｔ＝Ｔｆとの判定結果が得られる。各ランプの点灯状態がケース２に示す状態である場合には、Ｔａ＝Ｔであり当事者Ａの言い分が正しいとの判定結果が得られる。各ランプの点灯状態がケース３に示す状態である場合には、Ｔｂ＝Ｔであり当事者Ｂの言い分が正しいとの判定結果が得られる。各ランプの点灯状態がケース４に示す状態である場合には、改ざん装置１３０Ａ及び／又は改ざん装置１３０Ｂの挿入による不正操作の可能性があり、互いの文書について更に認証処理を行う必要があるとの判定結果が得られる。各ランプの点灯状態がケース５に示す状態である場合には、上記ケース２に該当する場合以外には、当事者Ｂ側で改ざん装置１３０Ｂの挿入等による不正操作の可能性があり、Ｔが正しい文書であるとの判定結果が得られる。各ランプの点灯状態がケース６に示す状態である場合には、上記ケース３に該当する場合以外には、当事者Ａ側で改ざん装置１３０Ａの挿入等による不正操作の可能性があり、Ｔｆが正しい文書であるとの判定結果が得られる。各ランプの点灯状態がケース７に示す状態である場合には、当事者Ａ，Ｂの双方の側で改ざん装置１３０Ａ又は１３０Ｂの挿入等による不正操作の可能性があり、Ｔ及びＴｆのいずれも正しい文書ではないとの判定結果が得られる。各ランプの点灯状態がケース８に示す状態である場合には、当事者Ａ，Ｂの双方ともに、文書Ｔａ、Ｔａｊ、Ｔｂ、Ｔｂｊのいずれに対しても電子印鑑を用いて押印した事実が存在しないとの判定結果が得られる。

【0111】

次に、電子印鑑同士の相互認証（情報交換による認証）について説明する。この場合、不正な目的で設置される改ざん装置の存在を考慮したうえでどちらの主張が正しいか検査しなければならない。例えば、当事者Ｂが不正な目的をもって改ざん装置１３０Ｂを電子印鑑１００Ｂ側に設置した場合、次のような状況が発生する。改ざん装置１３０Ｂが可能な動作は以下の表２に示す通りである。なお、当事者Ａが不正な目的をもって改ざん装置１３０Ａを設置した場合も同様である。

【0112】

【表2】

不正操作	Ａｉ	Ａｊ	Ｂｉ	Ｂｊ	ＬｉＡ	ＬｊＡ	ＬｉＢ	ＬｊＢ	Ｂにとって効果
Ｂに対して Ｔ⟷Ｔｆ	Ｔ	Ｔｆ	Ｔ	Ｔｆ	○	×	○	×	有り。認証が必要。
Ｂ Ｔｆ→Ｔ	Ｔ	Ｔｆ	Ｔ	Ｔ	○	×	○	○	無し（Ｔを正と判定）
Ｂ Ｔ→Ｔｆ	Ｔ	Ｔｆ	Ｔｆ	Ｔｆ	○	×	×	×	無し（Ｔを正と判定）
Ａに対して Ｔｆ→Ｔ	Ｔ	Ｔ	Ｔｆ	Ｔ	○	○	×	○	無し（Ｔを正と判定）

改ざん装置１３０Ｂが、ＴをＴｆに入れ替える（Ｔ⟷Ｔｆ）処理を行った場合に、当事者ＡとＢのどちらが不正目的の改ざん装置を設置しているかは、認証が終わるまでわからない。当事者Ｂによる押印そのものの否定は、当事者ＡがＩＤＡ、ＩｎｃｒＡ、ＩＤＢ、ＩｎｃｒＢに基づいて自己の電子印鑑１００Ａに蓄積した履歴情報の中から探し出した画像を視認することで確認が行われる。システムとして必ずしも本人認証を保証し得るものではないが、画像は真正なものであることが保証されるので、補強情報として利用できる。

【0113】

（ステップ１：データ交換）

電子印鑑１００ＡはＴａを自らが生成する使い捨て暗号鍵Ｋａにより暗号化して（Ｔａ）Ｋａを作成し、電子印鑑１００ＢはＴｂを自らが生成

する使い捨て暗号Ｋｂにより暗号化して（Ｔｂ）Ｋｂを作成し、電子印鑑１００Ａに送る。改ざん装置１３０ＢはＫａ、Ｋｂを知らないので、（Ｔａ）Ｋａ、（Ｔｂ）Ｋｂに代えて正しい（Ｔａ）Ｋａ、（Ｔｂ）Ｋｂを作ることができない。改ざん装置１３０Ｂができるのは伝送データを電子印鑑が不正であると判定するように改ざんすることだけである。電子印鑑１００Ａは（Ｔａ）ＫｂＫａを作成し、また電子印鑑１００Ｂは（Ｔｂ）ＫａＫｂを作成し、その後お互いに（Ｔａ）ＫｂＫａと（Ｔｂ）ＫａＫｂを交換する。両方のデータが一致すればＴａ＝Ｔｂであると電子印鑑１００Ａ、電子印鑑１００Ｂの双方が認証したことになる。ランプＬｊＡ、ランプＬｊＢがともに「正」状態に表示されるが、Ｔａ＝Ｔｂ＝Ｔが証明されたわけではない。しかしステップ１を省略すると電子印鑑１００Ｂは、電子印鑑１００Ａ側から「改ざん装置を入れているのではないか」との指摘がなされるとこれに反論できない。ステップ１は、当事者Ａ側の、ＴをＴｆに入れ替える（Ｔ←→Ｔｆ）操作は確実であると当事者Ｂに認めさせる効果がある。

【0114】

（ステップ２：Ｔａｊ≠Ｔｂであることを確認）

Ｔａｊを使用してステップ１の処理を行う。Ｔａｊ＝Ｔｆが送られたとき、ＬｉＢが「正」を示すはずである。しかし、ＬｊＢが「不正」を表示しても当事者Ｂの抱く疑いに対して反論できない。なお、本ステップの処理は省略も可能である。

【0115】

（ステップ３：Ｔａ＝Ｔであることを検査）

電子印鑑１００Ａは、内部に保存していたＴよりステップ１の処理を行う。このとき電子印鑑１００Ｂが主張するように、仮に電子印鑑１００Ａ側に改ざん装置１３０Ａが存在し、ＴａにＴｆを書き込んでいれば、Ｔを送ったとき、かならずＬｊＢは不正を示すはずである。Ｔａ＝Ｔｂ＝Ｔ、従って、Ｔｂ＝Ｔ≠Ｔｆであり、電子印鑑１００Ｂが正しくＴｆを読み込んでいることが否定される。電子印鑑１００Ｂ側に設置された改ざん装置１３０Ｂはこれを予想してＬｊＢを不正とするような動作をする。

【0116】

ＴａまたはＴを明示的に送っていると、改ざん装置が動作している可能性がある。そのためステップ１においてランダムにＴａとＴを送る。このときどちらを送ったか電子印鑑１００Ａは外部に出さない。電子印鑑１００ＢはＴａとＴｂのどちらが送られてきたかわからない状態で、ＬｊＢの状態を電子印鑑１００Ａに伝える。電子印鑑１００Ａは、ＬｆＡの状態は、Ｔを送った時に、ＬｊＢが正を表示したことを示し、お互いに（Ｔ）ＫｂＫａ、（Ｔｆ）ＫａＫｂを交換して等しくなるか確かめる。この時、Ｔａ＝Ｔｂ＝Ｔが確認される。この場合は、メーカに電子印鑑１００Ａと改ざん装置１３０Ｂのどちらがなりすましを行っているか検証してもらうこととなる。電子印鑑１００Ａはメーカの疑問を呼ばない。改ざん装置１３０Ｂはメーカの質問に答えるために電子印鑑１００Ｂの助けを借りる必要がある。メーカの質問は、電子印鑑１００Ｂしか復号できないＫｔｂを用いて行われる。改ざん装置はメーカによる検査の期間どうしても電子印鑑１００Ｂを接続しておかなければならない。このときメーカが当該ＴＩＤを持つＴを出力させる要求を行うと電子印鑑１００Ｂは該当するＴＩＤが入っていないので答えられない。改ざん装置１３０Ｂはこの質疑を察知できず、電子印鑑１００Ｂの回答を自らが蓄積しているＴＩＤに置き換えられない。

【0117】

第三者認証機関を利用すれば、公開鍵を使って、認証や伝送路の暗号化を行えるが、第三者の介入無しに契約文書の認証を行う場合、本実施形態のシステムは有効である。暗号化無しでは二者間で正しい押印認証が行えない。二者間で公開鍵方式を使うことにより文書の認証を行うことが可能であるが、この場合、どちらかに主導権があり、対等な状態での判定はできない。共通鍵方式では、全部の電子印鑑が同じ鍵を使うので、一度鍵が盗まれるとシステムが崩壊するおそれがある。本方式の認証は使い捨ての鍵しか使わず、システムが崩壊する可能性はきわめて低い。本方式でもＩｎｃｒＮの正当性を電子印鑑のメーカに依存するので、全く第三者の介入が無いわけではないが、一方が特定の方法でなりす

ましを行った場合のみメーカに検証を依頼すればよいので、大部分のトラブルについては二者間で解決できる。

【0118】

本実施形態のシステムの特徴をまとめると以下のようになる。

(1)当事者Ｂの否定に対する当事者Ａの反論

電子印鑑の使用についての否定（押印の否定）については、Ｖｂｉの提示によりこれを覆すことができる。

(2)Ｔｅｘｔｆの否定

文書番号の否定については、ＴＩＤＢによる電子印鑑１００Ｂの検索により、これを覆すことができる。

(3)電子印鑑１００Ａ、電子印鑑１００Ｂのもつ秘密

これから発生する未来のＩｎｃｒＮについて、電子印鑑のメーカだけが知り得る。

(4)誰も知り得ない事項

暗号鍵Ｋｉｎｃｒ、インサート（合成）前の自分の画像については誰も知り得ない。

(5)改ざんできない内容

ＴＩＤをインサート（合成）後の画像については改ざんできない。

(6)不変が保証されるもの

各電子印鑑のスタンプＩＤ（ＩＤＡ、ＩＤＡｂ）、各電子印鑑内に保存される文書Ｔについては不変であることが保証される。

(7)排除が保証されているもの

ＴＩＤＡは電子印鑑１００Ａ、１００Ｂ内の調印文書にでてくるのはただ１つである。ＴＩＤＢも電子印鑑１００Ａ、１００Ｂ内の調印文書にでてくるのはただ１つである。

(8)その他

ＩＤＡ、ＩｎｃｒＡ、ＩＤＢ、ＩｎｃｒＢが各電子印鑑の内部に保存された画像Ｖａｉ、Ｖｂｉの上でそろうことは、少なくとも電子印鑑１００Ａ、電子印鑑１００Ｂが利用されたことを示している（証明できる）。

【0119】

なお、本発明は上述した実施形態の内容に限定されるものではなく、本発明の要旨の範囲内において種々の変形実施が可能である。

【図面の簡単な説明】

【0120】

【図1】本発明を適用した一実施形態の電子認証システムの構成を説明する図である。

【図2】電子認証システムにおける認証処理の手順を説明するフローチャートである。

【図3】電子印鑑の具体例について説明する図（斜視図）である。

【図4】当事者のいずれも改ざん等の不正を行わない正常な状況における電子印鑑の使用時の構成例を示す図である。

【図5】当事者のいずれか（或いは双方とも）が改ざん等の不正を行う状況における電子印鑑の使用時の構成例を示す図である。

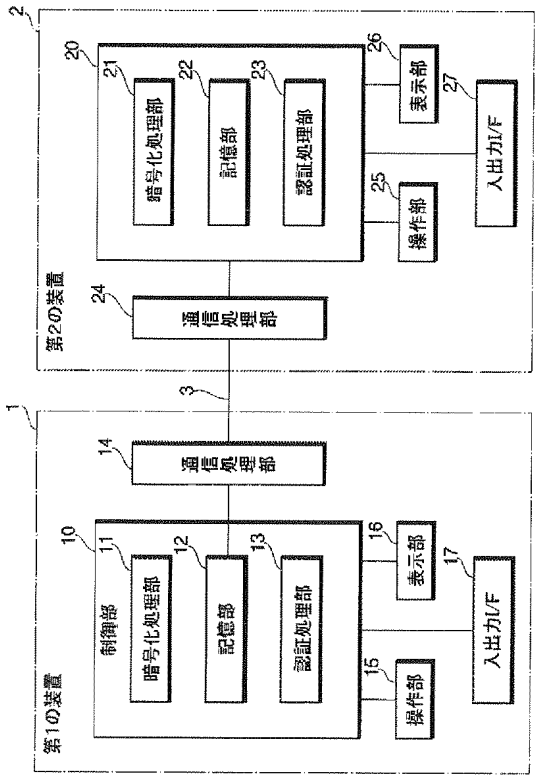
【符号の説明】

【0121】

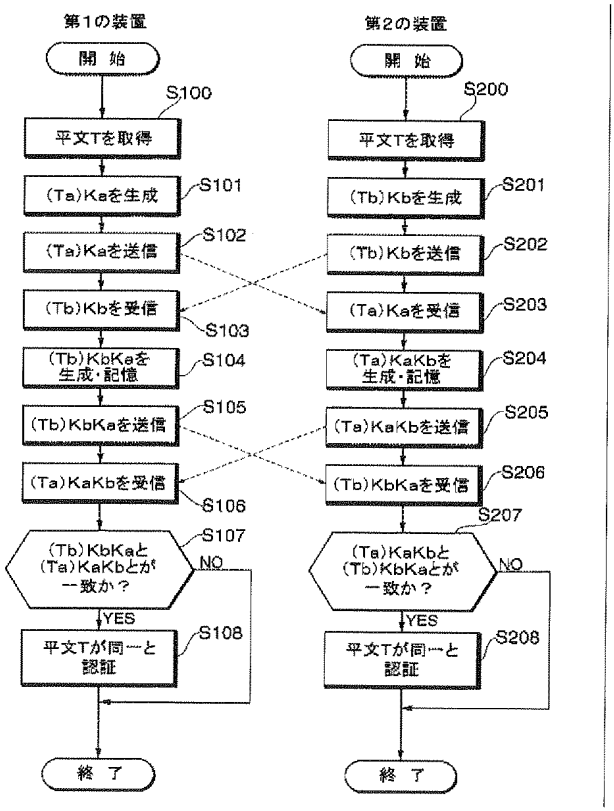
１…第１の装置
２…第２の装置
１０、２０…制御部
１１、２１…暗号化処理部
１２、２２…記憶部
１３、２３…認証処理部
１４、２４…通信処理部
１５、２５…操作部
１６、２６…表示部
１７、２７…入出力インタフェース

１００、１００Ａ、１００Ｂ…電子印鑑
１０１…操作キー（数字キー）
１０２～１０５…ランプ
１０６…カメラユニット
１０７…液晶表示部
１０８…入出力インタフェース

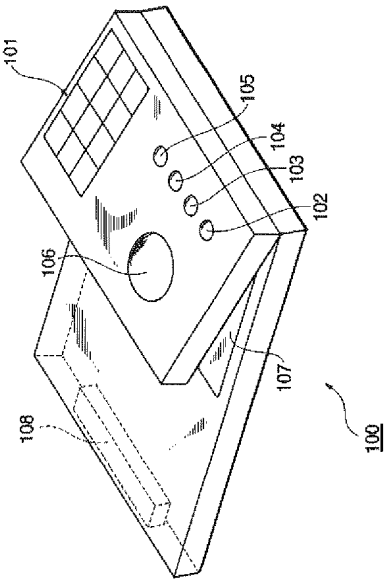
【図1】



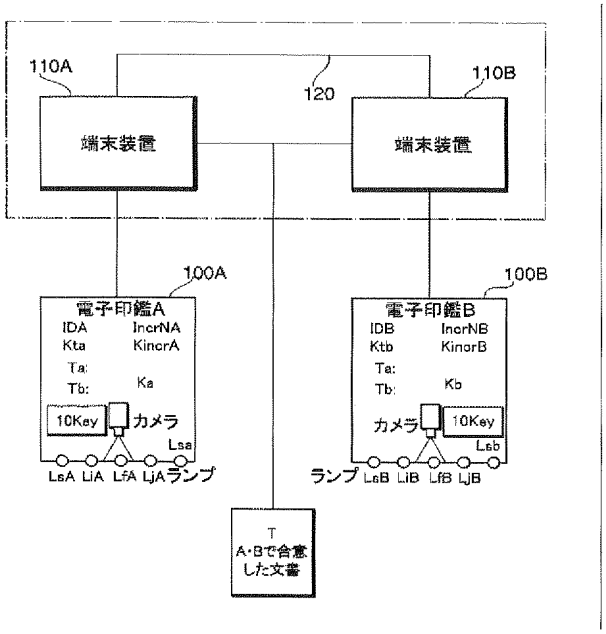
【図2】



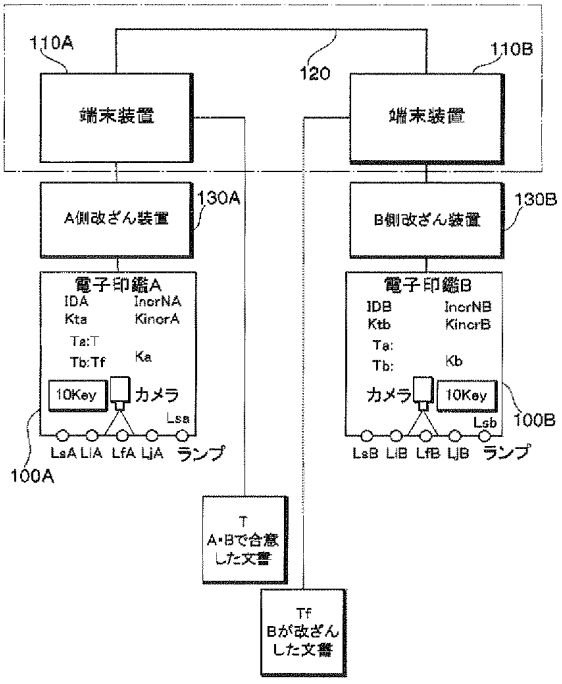
【図3】


101
105
104
103
102
106
107
108
100

【図4】


110A
120
110B
端末装置
端末装置
100A
100B
電子印鑑A
IDA
IncrNA
Kta
KincrA
Ta:
Tb:
Ka
10Key
カメラ
Lsa
LsA LiA LfA LjA ランプ
電子印鑑B
IDB
IncrNB
Ktb
KincrB
Ta:
Tb:
Kb
カメラ
10Key
Lsb
ランプ LsB LiB LfB LjB
T
A・Bで合意
した文書

【図5】


110A
120
110B
端末装置
端末装置
A側改ざん装置
130A
B側改ざん装置
130B
電子印鑑A
IDA
IncrNA
Kta
KincrA
Ta:T
Tb:Tf
Ka
10Key
カメラ
Lsa
LsA LiA LfA LjA ランプ
100A
電子印鑑B
IDB
IncrNB
Ktb
KincrB
Ta:
Tb:
Kb
カメラ
10Key
Lsb
LsB LiB LfB LjB ランプ
100B
T
A・Bで合意
した文書
Tf
Bが改ざん
した文書